US006523113B1

(12) **United States Patent**
Wehrenberg

(10) **Patent No.: US 6,523,113 B1**
(45) **Date of Patent: Feb. 18, 2003**

(54) **METHOD AND APPARATUS FOR COPY PROTECTION**

(75) Inventor: **Paul J. Wehrenberg**, Palo Alto, CA (US)

(73) Assignee: **Apple Computer, Inc.**, Cupertino, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/188,917**

(22) Filed: **Nov. 9, 1998**

Related U.S. Application Data

(60) Provisional application No. 60/088,654, filed on Jun. 9, 1998.

(51) **Int. Cl.**^{7} **H04L 9/00**; H04L 9/30
(52) **U.S. Cl.** **713/176**; 380/201; 380/203; 380/210; 380/30
(58) **Field of Search** 380/201, 203, 380/210; 713/176

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,613,004 A * 3/1997 Cooperman et al. 380/28
5,905,800 A * 5/1999 Moskowitz et al. 380/28
6,131,161 A * 10/2000 Linnartz 713/176
6,141,753 A * 10/2000 Zhao et al. 713/176

OTHER PUBLICATIONS

"Interim Report: Results of Phases I and II", Data Hiding SubGroup Copy Protection Technical Working Group, Version 1.0, May 26, 1998.

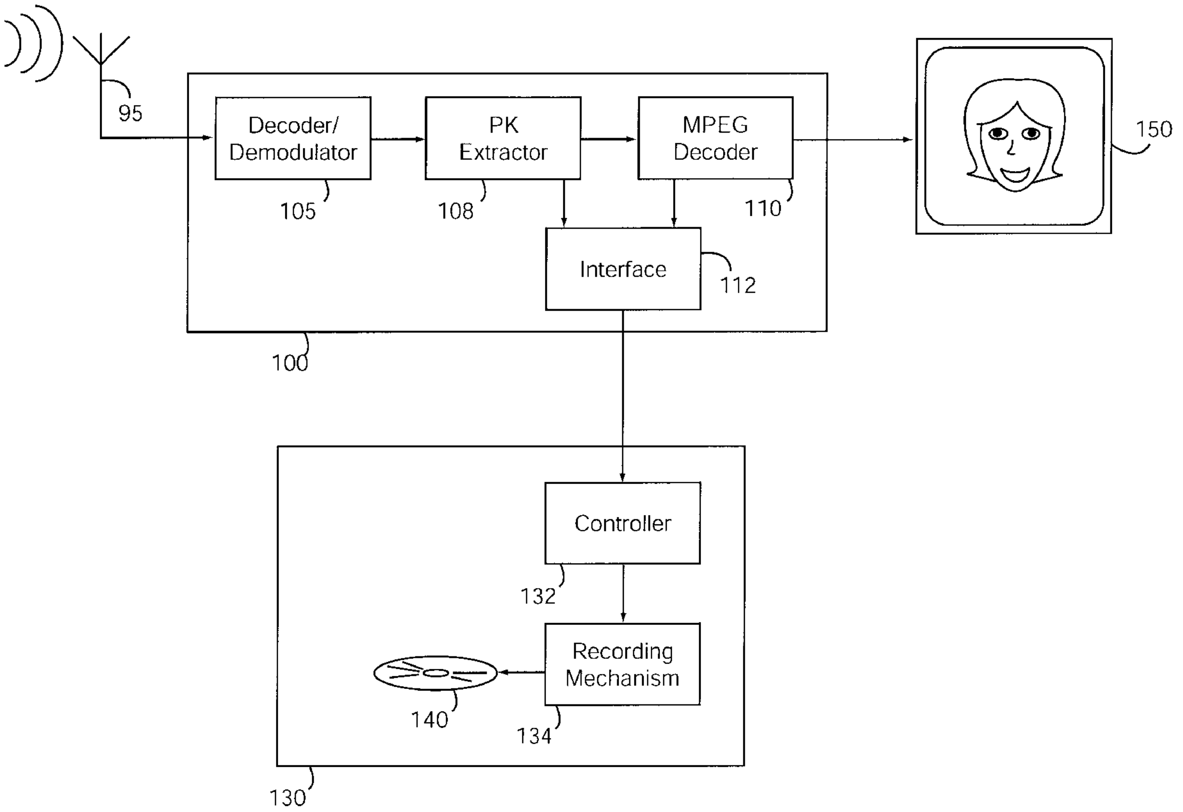
* cited by examiner

Primary Examiner—Gilberto Barrón
Assistant Examiner—Paul E. Callahan
(74) *Attorney, Agent, or Firm*—Beyer Weaver & Thomas, LLP

(57) **ABSTRACT**

Copy protection techniques that utilize a watermark and a permission key are disclosed. The copy protection techniques can provide single-copy copy protection in addition to different levels of copy protection. The permission key and the watermark can also permit the invention to yield variable levels of copy protection. In one embodiment, content including a watermark is transmitted to a recipient. The recipient is allowed to read the content but not record the content unless the recipient possesses a permission key.

18 Claims, 10 Drawing Sheets



US006457058B1

(12) **United States Patent**
Ullum et al.

(10) **Patent No.: US 6,457,058 B1**
(45) **Date of Patent: Sep. 24, 2002**

(54) **NETWORK SWITCH WITH HASH TABLE LOOK UP**

(75) Inventors: **Daniel Ullum**, San Jose; **Thomas J. Edsall**, Mountain View; **Soei-Shin Hang**, Sunnyvale, all of CA (US)

(73) Assignee: **Cisco Technology, Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/904,431**

(22) Filed: **Jul. 12, 2001**

Related U.S. Application Data

(63) Continuation of application No. 09/162,730, filed on Sep. 29, 1998, now Pat. No. 6,266,705.

(51) **Int. Cl.**^{7} **G06F 15/173**
(52) **U.S. Cl.** **709/238**; 709/245
(58) **Field of Search** 709/238, 245, 709/236; 711/216, 206, 208, 209, 205; 370/259, 401, 409, 392, 428, 474, 423, 360, 380, 381

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,305,317	A		4/1994	Szczepanek	
5,414,704	A		5/1995	Spinney	
5,740,171	A		4/1998	Mazzola et al.	
5,852,607	A		12/1998	Chin	
5,914,938	A		6/1999	Brady et al.	
6,034,957	A	*	3/2000	Haddock et al.	370/392
6,081,522	A		6/2000	Hendel et al.	
6,085,238	A		7/2000	Yuasa et al.	
6,098,110	A		8/2000	Witkowski et al.	
6,145,064	A	*	11/2000	Long et al.	711/158
6,266,705	B1	*	7/2001	Ullum et al.	709/238
6,295,299	B1	*	9/2001	Haddock et al.	370/423

OTHER PUBLICATIONS

Stallings, William, Data and Computer COmmunications, 5th Ed., 1997, pp. 640–642.
Perlman, RADIA Interconnections, 2nd Ed., 1999, pp. 141–143.

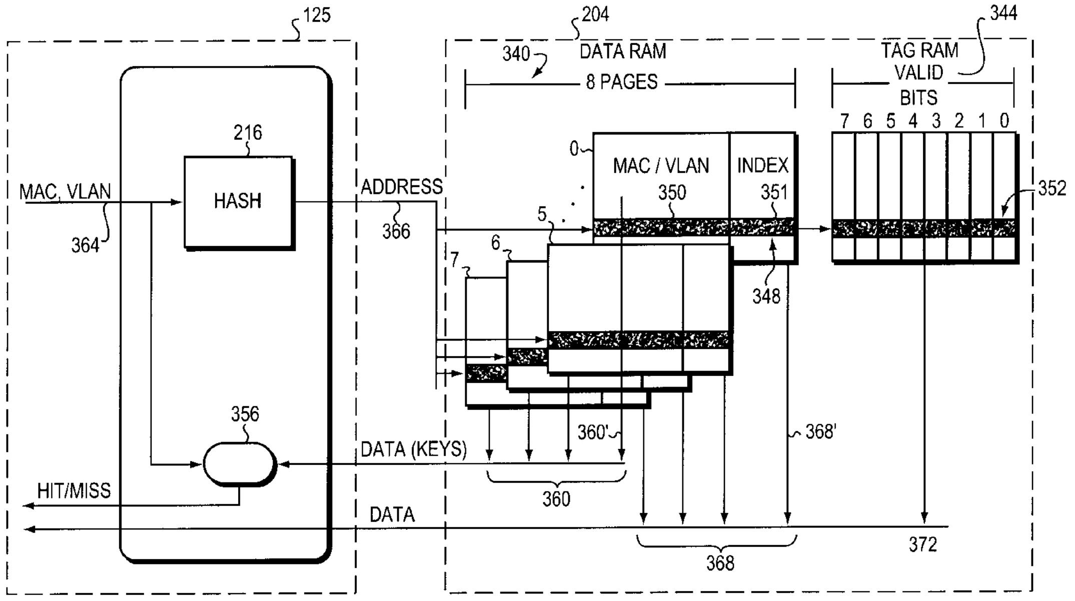
* cited by examiner

Primary Examiner—Mehmet B. Geckil
(74) *Attorney, Agent, or Firm*—Cesari and McKenna, LLP

(57) **ABSTRACT**

An improved look up mechanism for accessing a RAM to obtain forwarding information for data frames being transported among ports of a high-performance switch is provided. The look up mechanism includes a multi-page look up table and associated hashing technique. A media access control (MAC) address and a virtual local area network (VLAN) identifier are transformed with a hash function to obtain a hash key. The hash key is an address pointing to a particular entry in the look up table. A virtual first page is also derived from the hash key, which selects a particular physical page of the look up table to be initially accessed each time that MAC address/VLAN pair is used. The look up mechanism may also be used to access a short cut table containing Layer **3** short cut information. In either case, ultimately, the likelihood is increased that a match will be found on the first RAM access, thus maintaining high-speed switch performance.

23 Claims, 5 Drawing Sheets



US006978370B1

(12) United States Patent
Kocher

(10) Patent No.: **US 6,978,370 B1**
(45) Date of Patent: **Dec. 20, 2005**

(54) **METHOD AND SYSTEM FOR COPY-PREVENTION OF DIGITAL COPYRIGHT WORKS**

(75) Inventor: **Paul C. Kocher**, San Francisco, CA (US)

(73) Assignee: **Cryptography Research, Inc.**, San Francisco, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/274,496**

(22) Filed: **Mar. 23, 1999**

Related U.S. Application Data

(60) Continuation of application No. 08/882,511, filed on Jun. 25, 1997, now abandoned, which is a division of application No. 08/707,289, filed on Sep. 3, 1996, now abandoned.

(51) **Int. Cl.**^{7} **H04L 9/00**
(52) **U.S. Cl.** **713/176**; 380/201
(58) **Field of Search** 713/193, 161, 713/176, 168; 705/51, 57–59; 380/201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,598,288	A		7/1986	Yarbrough et al.	
5,315,448	A		5/1994	Ryan	
5,323,244	A		6/1994	Yamaguchi et al.	
5,343,527	A		8/1994	Moore	380/4
5,418,853	A		5/1995	Kanota et al.	380/5
5,450,489	A		9/1995	Ostrover et al.	380/3
5,513,260	A		4/1996	Ryan	380/3
5,574,787	A		11/1996	Ryan	380/5
5,590,194	A		12/1996	Ryan	380/5
5,606,612	A		2/1997	Griffin et al.	380/14
5,613,004	A	*	3/1997	Cooperman et al.	380/28
5,646,999	A		7/1997	Saito	380/25
5,687,236	A		11/1997	Moskowitz et al.	380/28
5,822,436	A	*	10/1998	Rhoads	380/54
5,862,218	A	*	1/1999	Steinberg	713/176

FOREIGN PATENT DOCUMENTS

EP	0717337 A1	*	6/1994	G06F 12/14

OTHER PUBLICATIONS

Gustavus Simmons Contemporary Cryptology, IEEE Press 1991.*

Lecture Notes in Computer Science, Ross Anderson (Ed.), “Information Hiding,” First International Workshop, Cambridge, U.K., May 30-Jun. 1, 1996 Proceedings, Springer.

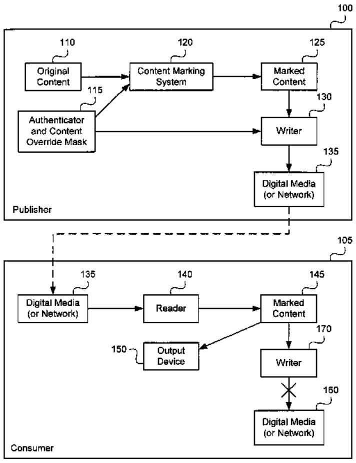
* cited by examiner

Primary Examiner—Kim Vu
Assistant Examiner—Thanhnga Truong
(74) *Attorney, Agent, or Firm*—Sonnenschein Nath & Rosenthal LLP

(57) **ABSTRACT**

Methods and apparati for marking digital material and for detecting marks therein. For mark detection, the material is divided into a plurality of blocks, to which a non-collision resistant compression function is applied. Compression outputs are placed in a shift register, whose value is tested for predetermined values or patterns. Mark embedding may be performed by modifying the data (for example by altering low-order bits and other non-critical regions) such that the outputs of the compression operation, when used as an input to the shift register, yield a predetermined value or pattern. A Hamming Majority operation, computed as the most common bit in a block, may be used as the compression operation, enabling marking and mark detection with material of virtually all types and formats. Mark detection technology may be implemented in media writers and other devices to determine whether the digital material is copyrighted or otherwise protected. An override capability is provided to allow authorized parties to bypass the protection.

10 Claims, 10 Drawing Sheets



US005530751A

United States Patent [19]

Morris

[11] **Patent Number: 5,530,751**

[45] **Date of Patent: Jun. 25, 1996**

[54] **EMBEDDED HIDDEN IDENTIFICATION CODES IN DIGITAL OBJECTS**

[75] Inventor: **Dale C. Morris**, Menlo Park, Calif.

[73] Assignee: **Hewlett-Packard Company**, Palo Alto, Calif.

[21] Appl. No.: **269,807**

[22] Filed: **Jun. 30, 1994**

[51] **Int. Cl.**^{6} **H04L 9/00**

[52] **U.S. Cl.** **380/4**

[58] **Field of Search** 380/4, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,609,697	9/1971	Blevins et al.	380/4
4,120,030	10/1978	Johnstone	380/4
4,658,093	4/1987	Hellman	380/4
5,208,853	5/1993	Armbruster et al.	380/4
5,212,728	5/1993	Glover et al.	380/4
5,293,422	5/1994	Loiacono	380/4
5,371,792	12/1994	Asai et al.	380/4
5,398,285	5/1995	Borgelt et al.	380/4

FOREIGN PATENT DOCUMENTS

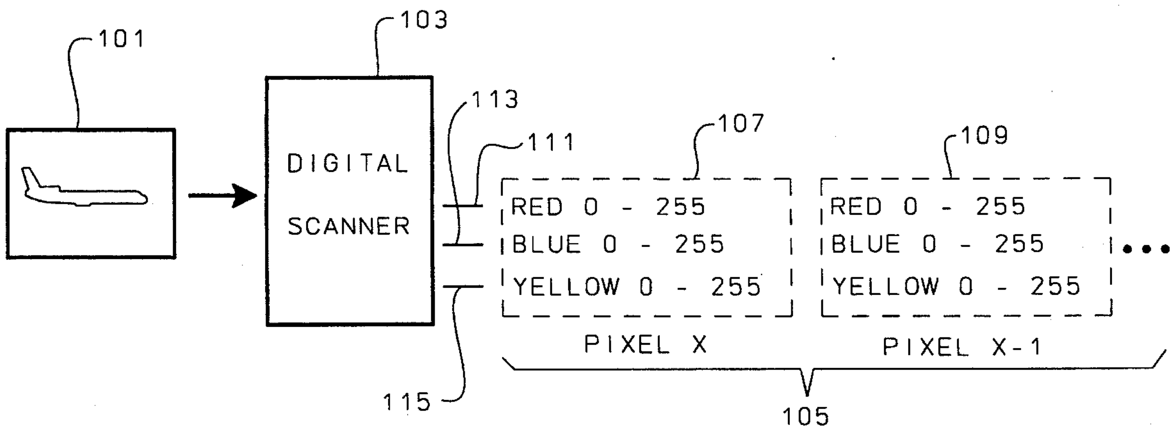
0366381	10/1989	European Pat. Off. .
0418964	9/1990	European Pat. Off. .
0496607	1/1992	European Pat. Off. .
0580367	7/1993	European Pat. Off. .
0589459	9/1993	European Pat. Off. .
WO92/16944	1/1992	WIPO .

Primary Examiner—Salvatore Cangialosi
Attorney, Agent, or Firm—Howard R. Boyle

[57] **ABSTRACT**

A method and apparatus for encoding identification information into a stream of digital data representing an object. The digital data representing an object is modified to add embedded identification information into the data. This modification is done such that the resultant changes to the object are not objectionable to the user. By comparing the original digital data to the modified data, the possessor of the original data can recover the embedded identification information. However the identification information is effectively unavailable to anyone not possessing the original data.

8 Claims, 10 Drawing Sheets



US006823455B1

(12) **United States Patent**
Macy et al.

(10) **Patent No.: US 6,823,455 B1**
(45) **Date of Patent: Nov. 23, 2004**

(54) **METHOD FOR ROBUST WATERMARKING OF CONTENT**

(75) Inventors: **William W. Macy**, Palo Alto, CA (US); **Matthew J. Holliman**, Libertyville, IL (US); **Minerva Ming-Yee Yeung**, Sunnyvale, CA (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/288,836**

(22) Filed: **Apr. 8, 1999**

(51) **Int. Cl.**^{7} **H04L 9/00**; H04K 1/00; G09C 3/00; G09C 5/00

(52) **U.S. Cl.** **713/176**; 380/38; 380/54

(58) **Field of Search** 713/176; 380/54, 380/28

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,768,426	A	*	6/1998	Rhoads	382/232
5,905,800	A	*	5/1999	Moskowitz et al.	380/28
5,949,885	A	*	9/1999	Leighton	380/54
5,960,081	A	*	9/1999	Vynne et al.	713/176
6,272,634	B1	*	8/2001	Tewfik et al.	713/176

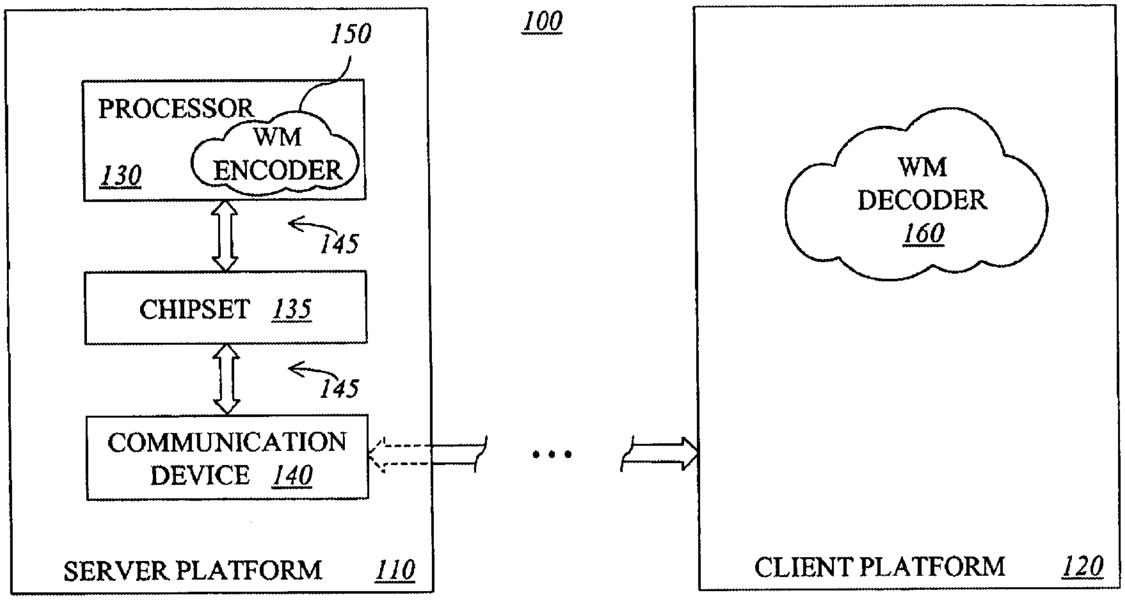
* cited by examiner

Primary Examiner—Gilberto Barrón
Assistant Examiner—Benjamin E. Lanier
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

(57) **ABSTRACT**

One inventive aspect pertains to a watermarking mechanism that allows a watermark to be determined from only a part of the video sequence without human intervention and without reference to the original watermarked frames. This watermark has improved invisibility, detection reliability and robustness. Invisibility is improved through the inclusion of frame difference parameters to calculate the amplitude of the watermark. Detection reliability and robustness can be improved by assuring that opposite signed values for the pseudo-random number sequence are spatially near each other and using data blocks forming the data sets, respectively. Another inventive aspect pertains to a watermarking mechanism that is exclusively dependent on the data contained in the data sets and is completely interoperable between spatial and compressed domains.

2 Claims, 9 Drawing Sheets



US006668246B1

(12) **United States Patent**
Yeung et al.

(10) **Patent No.: US 6,668,246 B1**
(45) **Date of Patent: Dec. 23, 2003**

(54) **MULTIMEDIA DATA DELIVERY AND PLAYBACK SYSTEM WITH MULTI-LEVEL CONTENT AND PRIVACY PROTECTION**

(75) Inventors: **Minerva Ming-Yee Yeung**, Sunnyvale, CA (US); **Matthew J. Holliman**, Libertyville, IL (US); **Robert G. Liu**, Sunnyvale, CA (US); **William W. Macy**, Palo Alto, CA (US); **Boon-Lock Yeo**, Sunnyvale, CA (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/275,905**

(22) Filed: **Mar. 24, 1999**

(51) **Int. Cl.**^{7} **G06F 17/60**
(52) **U.S. Cl.** **705/57**; 380/211; 705/1; 705/51; 713/150
(58) **Field of Search** 380/200, 201, 380/211; 705/1, 50, 51, 52, 54, 57; 713/150

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,933,971 A	*	6/1990	Bestock et al.	....	380/44
5,638,448 A	*	6/1997	Nguyen	....	380/29
5,689,566 A	*	11/1997	Nguyen	....	713/155
6,275,939 B1	*	8/2001	Garrison	....	713/200
6,298,446 B1	*	10/2001	Schreiber et al.	....	713/201
6,304,969 B1	*	10/2001	Wasserman et al.	....	713/172
6,353,892 B2	*	3/2002	Schreiber et al.	....	713/201

FOREIGN PATENT DOCUMENTS

JP	2000-148689 A	*	5/2000

OTHER PUBLICATIONS

Bobrowski: "Database in a client/server world—Understanding the unique challenges of keeping your client/server database environment secure"; DBMS, Sep. 1, 1994, vol. 7, No. 10, pp. 48–48, (Abstract Only).*

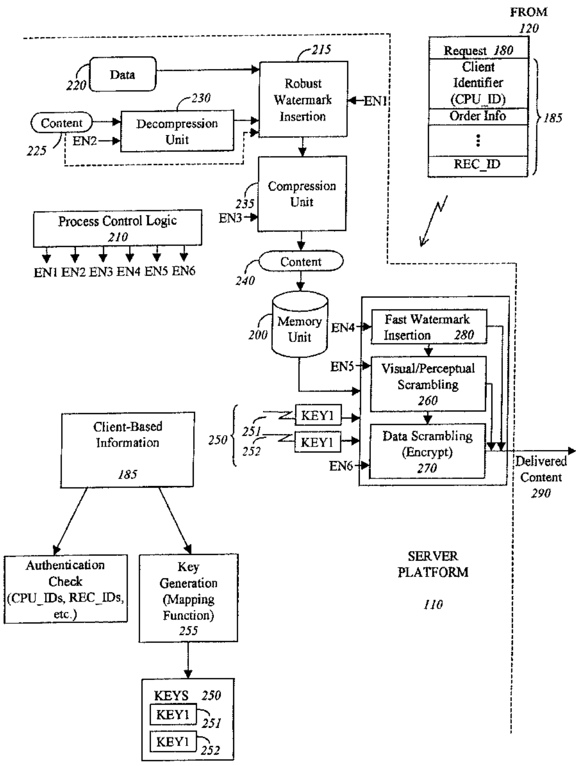
* cited by examiner

Primary Examiner—Edward R. Cosimano
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

(57) **ABSTRACT**

A content distribution system comprising a server platform and a client platform. The server platform includes a memory unit to store digital content and access control logic to activate content protection mechanisms that provide multiple levels of access protection to the digital content. In communication with the server platform, the client platform plays back segments of the digital content at one of a plurality of quality levels.

24 Claims, 9 Drawing Sheets



US006282650B1

(12) **United States Patent**
Davis

(10) **Patent No.: US 6,282,650 B1**
(45) **Date of Patent: Aug. 28, 2001**

(54) **SECURE PUBLIC DIGITAL WATERMARK**

(75) Inventor: **Derek L. Davis**, Phoenix, AZ (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/237,323**

(22) Filed: **Jan. 25, 1999**

(51) **Int. Cl.**^{7} **H04L 9/32**; H04L 1/44; G06F 12/14

(52) **U.S. Cl.** **713/176**; 713/193; 380/246; 380/282

(58) **Field of Search** 713/172, 176, 713/193, 194; 380/46, 51, 54, 55, 243, 246, 282, 285

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,138,196		2/1979	Redman	356/350
4,296,326		10/1981	Haslop et al.	250/372
4,754,327		6/1988	Lippert	358/88
5,118,526		6/1992	Allen et al.	427/161
5,267,042		11/1993	Tsuchiya et al.	358/209
5,568,552		10/1996	Davis	380/4
5,604,529		2/1997	Kuga et al.	348/46
5,636,362		6/1997	Stone et al.	395/456
5,659,195		8/1997	Kaiser et al.	257/415
5,664,018		9/1997	Leighton	380/54
5,675,654	*	10/1997	Ryan	380/48
5,687,236		11/1997	Moskowitz et al.	380/28
5,822,432		10/1998	Moskowitz et al.	380/28
5,825,892		10/1998	Braudaway et al.	380/51
5,848,155		12/1998	Cox	380/4
5,875,249		2/1999	Mintzer et al.	380/54
6,131,162	*	10/2000	Yoshiura et al.	713/176

FOREIGN PATENT DOCUMENTS

0 555 715 A1	8/1993	(EP)	G06F/12/14

OTHER PUBLICATIONS

Schneier, B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, Oct. 18, 1995, pp. 31–34.*

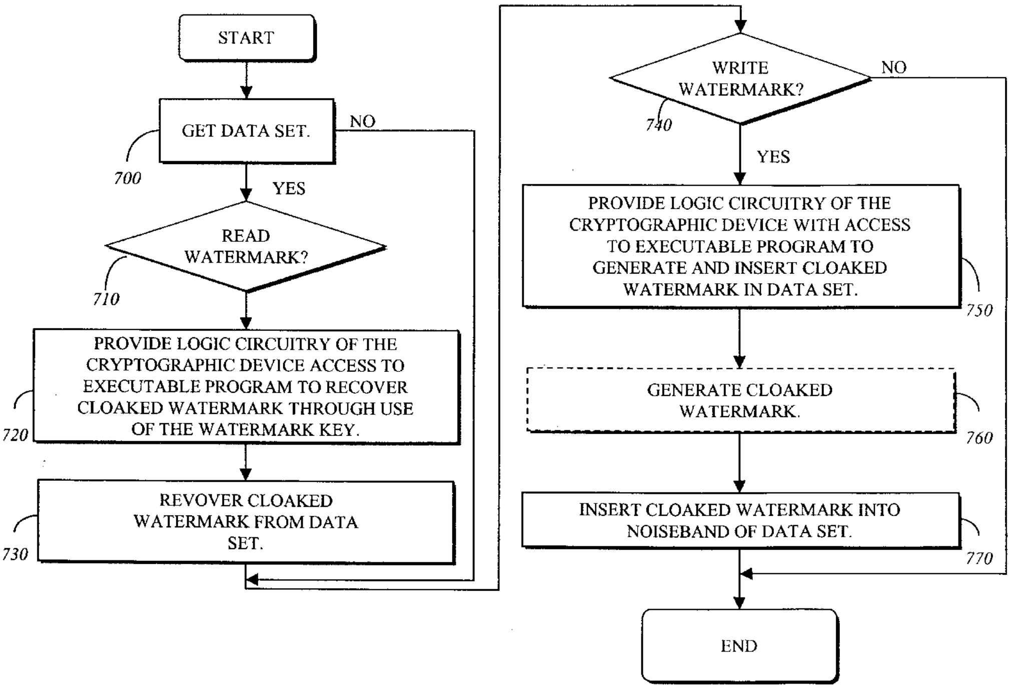
* cited by examiner

Primary Examiner—Tod Swann
Assistant Examiner—Justin T. Darrow
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

(57) **ABSTRACT**

A cryptographic device and corresponding method for producing a cloaked watermark which is a private watermark having the functionality of a public watermark. In one embodiment, the cryptographic device comprises an internal memory and a processor contained in a package. The internal memory provides a region for storage of key information used at least to produce the cloaked watermark. The processor is coupled to the internal memory and is responsible for producing a cloaked watermark based on the key and for inserting the cloaked watermark into an outgoing data set.

20 Claims, 5 Drawing Sheets


START
GET DATA SET.
700
NO
YES
READ WATERMARK?
710
PROVIDE LOGIC CIRCUITRY OF THE CRYPTOGRAPHIC DEVICE ACCESS TO EXECUTABLE PROGRAM TO RECOVER CLOAKED WATERMARK THROUGH USE OF THE WATERMARK KEY.
720
REVOVER CLOAKED WATERMARK FROM DATA SET.
730
WRITE WATERMARK?
740
NO
YES
PROVIDE LOGIC CIRCUITRY OF THE CRYPTOGRAPHIC DEVICE WITH ACCESS TO EXECUTABLE PROGRAM TO GENERATE AND INSERT CLOAKED WATERMARK IN DATA SET.
750
GENERATE CLOAKED WATERMARK.
760
INSERT CLOAKED WATERMARK INTO NOISEBAND OF DATA SET.
770
END

US005633932A

United States Patent [19]

Davis et al.

[11] **Patent Number: 5,633,932**

[45] **Date of Patent: May 27, 1997**

[54] **APPARATUS AND METHOD FOR PREVENTING DISCLOSURE THROUGH USER-AUTHENTICATION AT A PRINTING NODE**

[75] Inventors: **Derek L. Davis**, Phoenix; **Lionel Smith**, Queen Creek, both of Ariz.

[73] Assignee: **Intel Corporation**, Santa Clara, Calif.

[21] Appl. No.: **574,843**

[22] Filed: **Dec. 19, 1995**

[51] **Int. Cl.**^{6} **H04L 9/32**; H04L 9/00; B41J 29/54

[52] **U.S. Cl.** **380/25**; 380/3; 380/4; 380/23; 380/30; 380/49; 380/51; 380/55; 340/825.31; 340/825.34

[58] **Field of Search** 380/3, 4, 23, 25, 380/30, 49, 50, 51, 55, 59; 340/825.31, 825.34

[56] **References Cited**

U.S. PATENT DOCUMENTS

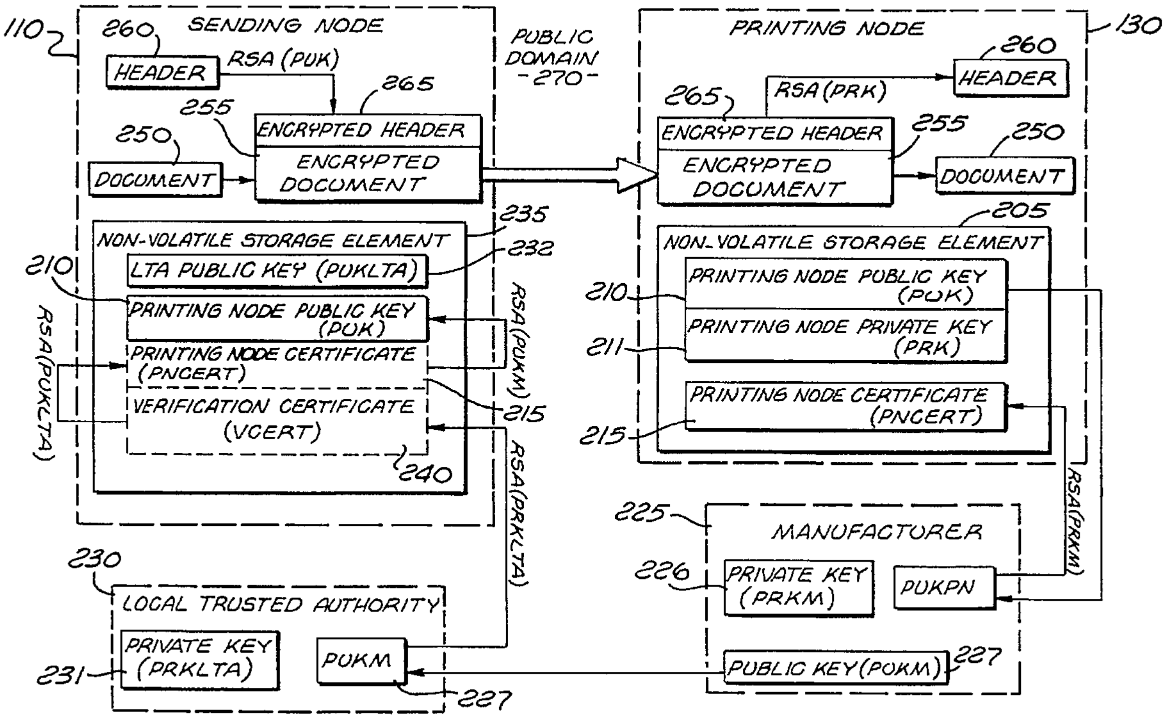
4,961,224	10/1990	Yung	380/25
5,509,074	4/1996	Choudhury et al.	380/23

Primary Examiner—Bernarr E. Gregory
Attorney, Agent, or Firm—Blakely, Sokoloff, Taylor & Zafman

[57] **ABSTRACT**

A system and method for preventing a copy of a document to the output from a printing node until the printing node authenticates the intended recipient. The system includes a sending node, a printing node and a communication link coupling these nodes together in a network fashion. The sending node has access to a public key of the printing node and uses this public key to encrypt a header and document before transmission to the printing node over the communication link. The priority node has access to its private key to decrypt the header to ascertain whether the document requires authentication by the intended recipient before being output.

24 Claims, 4 Drawing Sheets



US006785815B1

(12) **United States Patent**
Serret-Avila et al.

(10) **Patent No.: US 6,785,815 B1**
(45) **Date of Patent: Aug. 31, 2004**

(54) **METHODS AND SYSTEMS FOR ENCODING AND PROTECTING DATA USING DIGITAL SIGNATURE AND WATERMARKING TECHNIQUES**

(75) Inventors: **Xavier Serret-Avila**, Santa Clara, CA (US); **Gilles Boccon-Gibod**, Los Altos, CA (US)

(73) Assignee: **InterTrust Technologies Corp.**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 953 days.

(21) Appl. No.: **09/588,652**

(22) Filed: **Jun. 7, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/138,171, filed on Jun. 8, 1999.

(51) **Int. Cl.**^{7} **G06F 1/26**

(52) **U.S. Cl.** **713/176**; 713/182; 713/200; 713/201

(58) **Field of Search** 713/176, 182, 713/189, 200, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,827,508	A	5/1989	Shear
5,513,260	A	4/1996	Ryan
5,613,004	A	3/1997	Cooperman et al.
5,636,292	A	6/1997	Rhoads
5,659,613	A	8/1997	Copeland et al.
5,671,389	A	9/1997	Saliba

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

AU	A-36840/97	2/1998
EP	0 750423 A2	12/1996
EP	0 845 758 A2	6/1998
EP	0 903 943 A2	3/1999
WO	WO 98/10381	3/1998
WO	WO 99/48296	9/1999
WO	WO 00/44131	7/2000

OTHER PUBLICATIONS

Marc Schneider, et al., *A Robust Content Based Digital Signature for Image Authentication,* Proceedings of the International Conference on Image Processing, IEEE, Sep. 26, 1996, pp. 227–230.

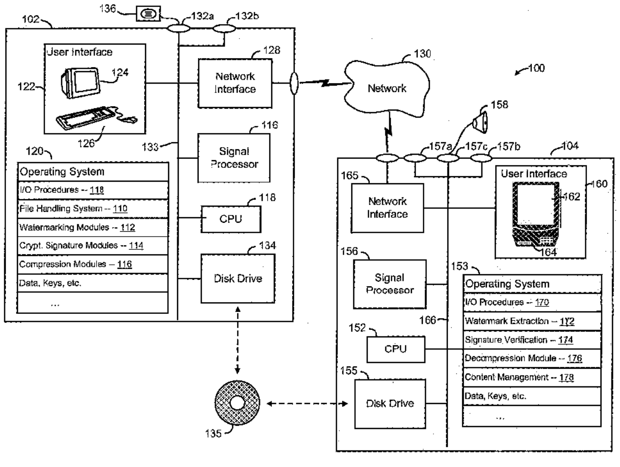
(List continued on next page.)

Primary Examiner—Thomas R. Peeso
(74) *Attorney, Agent, or Firm*—Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.

(57) **ABSTRACT**

Systems and methods are provided for protecting and managing electronic data signals that are registered in accordance with a predefined encoding scheme, while allowing access to unregistered data signals. In one embodiment a relatively hard-to-remove, easy-to-detect, strong watermark is inserted in a data signal. The data signal is divided into a sequence of blocks, and a digital signature for each block is embedded in the signal via a watermark. The data signal is then stored and distributed on, e.g., a compact disc, a DVD, or the like. When a user attempts to access or use a portion of the data signal, the signal is checked for the presence of a watermark containing the digital signature for the desired portion of the signal. If the watermark is found, the digital signature is extracted and used to verify the authenticity of the desired portion of the signal. If the signature-containing watermark is not found, the signal is checked for the presence of the strong watermark. If the strong watermark is found, further use of the signal is inhibited, as the presence of the strong watermark, in combination with the absence or corruption of the signature-containing watermark, provides evidence that the signal has been improperly modified. If, on the other hand, the strong mark is not found, further use of the data signal can be allowed, as the absence of the strong mark indicates that the data signal was never registered with the signature-containing watermark.

46 Claims, 20 Drawing Sheets



US005943422A

United States Patent [19]

Van Wie et al.

[11] **Patent Number: 5,943,422**

[45] **Date of Patent: Aug. 24, 1999**

[54] **STEGANOGRAPHIC TECHNIQUES FOR SECURELY DELIVERING ELECTRONIC DIGITAL RIGHTS MANAGEMENT CONTROL INFORMATION OVER INSECURE COMMUNICATION CHANNELS**

[75] Inventors: **David M. Van Wie**, Sunnyvale; **Robert P. Weber**, Menlo Park, both of Calif.

[73] Assignee: **InterTrust Technologies Corp.**, Sunnyvale, Calif.

[21] Appl. No.: **08/689,606**

[22] Filed: **Aug. 12, 1996**

[51] **Int. Cl.**^{6} **H04N 7/167**

[52] **U.S. Cl.** **380/9**; 380/5

[58] **Field of Search** 380/9, 20, 4, 5, 380/28; 382/232

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,573,747	4/1971	Adams et al. .
3,609,697	9/1971	Blevins .
3,796,830	3/1974	Smith .
3,798,359	3/1974	Feistel .
3,798,360	3/1974	Feistel .
3,798,605	3/1974	Feistel .
3,806,882	4/1974	Clarke .

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

9 004 79	12/1984	Belgium .
0 84 441	7/1983	European Pat. Off. .
A0135422	3/1985	European Pat. Off. .
0180460	5/1986	European Pat. Off. .
0 370 146	11/1988	European Pat. Off. .
0 456 386 A2	11/1991	European Pat. Off. .
0 469 864 A2	11/1991	European Pat. Off. .

(List continued on next page.)

OTHER PUBLICATIONS

Baum, Michael, Worldwide Electronic Commerce: Law, Policy and Controls Conference, program details, Nov. 11, 1993.

Bisbey, II et al., Encapsulation: An Approach to Operating System Security, Oct. 1973, pp. 666–675.

Blom et al., Encryption Methods in Data Networks, Ericsson Technics, No. 2, 1978, Stockholm, Sweden.

Bruner, Rick, E., PowerAgent, NetBot help advertisers reach Internet shoppers, Aug. 1997 (Document from Internet).

Cable Television and America's Telecommunications Infrastructure, National Cable Television Association, Apr. 1993.

Caruso, Technology, Digital Commerce 2 plans for watermarks, which can bind proof of authorship to electronic works, New York Times (Aug. 1995).

CD ROM, Introducing . . . The Workflow CD–ROM Sampler, Creative Networks, MCIMail: Creative Networks, Inc., Palo Alto, California.

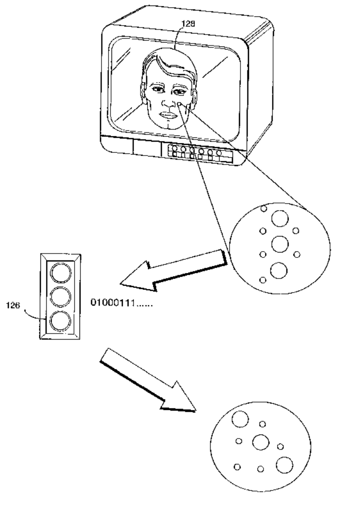
(List continued on next page.)

Primary Examiner—David Cain
Attorney, Agent, or Firm—Nixon & Vanderhye P.C.

[57] **ABSTRACT**

Electronic steganographic techniques can be used to encode a rights management control signal onto an information signal carried over an insecure communications channel. Steganographic techniques ensure that the digital control information is substantially invisibly and substantially indelibly carried by the information signal. These techniques can provide end-to-end rights management protection of an information signal irrespective of transformations between analog and digital. An electronic appliance can recover the control information and use it for electronic rights management to provide compatibility with a Virtual Distribution Environment. In one example, the system encodes low data rate pointers within high bandwidth time periods of the content signal to improve overall control information read/seek times.

348 Claims, 30 Drawing Sheets



EXAMPLE STEGANOGRAPHICALLY ENCODING ELECTRONIC CONTENTS IN AN IMAGE

US006381747B1

(12) United States Patent
Wonfor et al.

(10) Patent No.: US 6,381,747 B1
(45) Date of Patent: Apr. 30, 2002

(54) **METHOD FOR CONTROLLING COPY PROTECTION IN DIGITAL VIDEO NETWORKS**

(75) Inventors: **Peter J. Wonfor**, El Granada; **Derek T. Nelson**, Menlo Park, both of CA (US)

(73) Assignee: **Macrovision Corp.**, Sunnyvale, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/142,039**

(22) PCT Filed: **Mar. 31, 1997**

(86) PCT No.: **PCT/US97/05257**

§ 371 Date: **Aug. 31, 1998**

§ 102(e) Date: **Aug. 31, 1998**

(87) PCT Pub. No.: **WO97/37492**

PCT Pub. Date: **Oct. 9, 1997**

Related U.S. Application Data

(60) Provisional application No. 60/014,684, filed on Apr. 1, 1996.

(51) **Int. Cl.**^{7} **H04N 7/173**

(52) **U.S. Cl.** **725/104**; 386/94; 380/201; 380/203

(58) **Field of Search** 348/3, 5.5, 7, 10, 348/12; 386/1, 94; 360/60; 380/201, 203, 204; 725/104, 8, 30, 146, 1, 2, 31, 25

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,631,603	A	*	12/1986	Ryan	360/37.1
4,890,319	A	*	12/1989	Seth-Smith et al.	380/5
4,914,694	A	*	4/1990	Leonard et al.	380/5
5,315,448	A		5/1994	Ryan	
5,418,853	A	*	5/1995	Kanota et al.	380/5
5,574,787	A	*	11/1996	Ryan	380/5
5,654,747	A	*	8/1997	Ottesen et al.	348/12
5,675,647	A	*	10/1997	Garneau et al.	380/20
5,680,457	A	*	10/1997	Bestler et al.	380/21
5,737,417	A	*	4/1998	Buynak et al.	380/5
6,002,694	A	*	12/1999	Yoshizawa et al.	370/486
6,002,830	A	*	12/1999	Quan	386/1
RE36,763	E	*	7/2000	Kanota et al.	380/5

FOREIGN PATENT DOCUMENTS

EP	0691787	1/1996

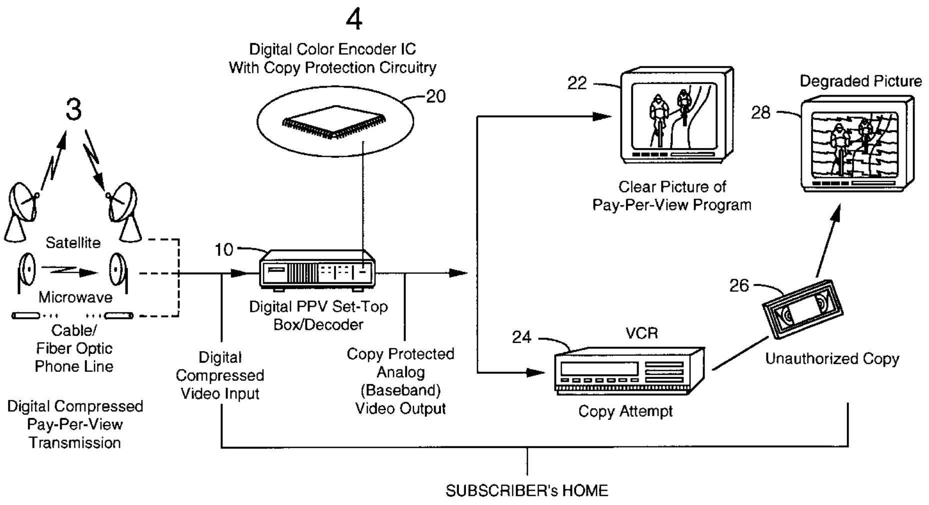
* cited by examiner

Primary Examiner—Andrew Faile
Assistant Examiner—Ngoc Vu
(74) *Attorney, Agent, or Firm*—George Almeida; Frank Nguyen

(57) **ABSTRACT**

A method and system of providing copy protection of video analog and digital signals and the like, wherein the signals are transmitted via a digital delivery network, and may comprise, for example, pay per view (PPV) program materials protected by copyrights of respective program rights holders. The right holders authorize video service providers (**3**) to apply copy protection to the program material. The copy protection process is supplied to the rights holders or the service providers (**3**) by a copy protection process licensor. The video service providers (**3**) supply suitable copy protection control software via respective control and billing (tracking) centers to generate commands which activate, control and reconfigure the copy protection process being applied to the programs being transmitted. A settop box (**10**) is provided to each consumer and contains a copy protection circuit which is adapted to apply selected anti-copy waveforms to the video signal corresponding to the program material in response to the commands from the service providers (**3**). Usage data pertinent to each consumer is returned by the settop box (**10**) to the service providers (**3**), which then report the copy protection usage to the respective rights holders and process licensor.

52 Claims, 3 Drawing Sheets



US006049838A

United States Patent [19]

Miller et al.

[11] **Patent Number: 6,049,838**

[45] **Date of Patent: Apr. 11, 2000**

[54] **PERSISTENT DISTRIBUTED CAPABILITIES**

[75] Inventors: **Mark S. Miller**, Los Altos; **Norman Hardy**, Portola Valley; **E. Dean Tribble**, Los Altos Hills; **Christopher T. Hibbert**, Mountain View; **Eric C. Hill**, Palo Alto, all of Calif.

[73] Assignee: **Sun Microsystems, Inc.**, Mountain View, Calif.

[21] Appl. No.: **08/673,058**

[22] Filed: **Jul. 1, 1996**

[51] **Int. Cl.**^{7} **G06F 15/163**; G06F 9/00; G06F 9/46

[52] **U.S. Cl.** **709/303**; 380/49

[58] **Field of Search** 395/680, 682, 395/683; 709/300, 302, 303, 229; 380/23, 24, 25, 49

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,027,269	6/1991	Grant et al.	395/680
5,446,901	8/1995	Owicki et al.	711/154
5,603,031	2/1997	White et al.	395/683

OTHER PUBLICATIONS

Codie Wells: A Note on “Protection Imperfect” (1988) 2 pages.

Marc Shapiro, et. al.: Some Key Issues in the Design of Distributed Garbage Collection and References (Apr. 15, 1994) pp. 1–13.

M. Anderson, et al.: A Password–Capability System (1986) The Computer Journal, vol. 29, No. 1.

Andrew Birrell, et al.: Network Objects (SRC Research Reports #115) (Feb. 28, 1994) pp. 1–65.

Andrew Birrell, et al.: Distributed Garbage Collection for Network Objects (SRC Research Report #116) pp. 1–18.

Norm Hardy, The Confused Deputy (1985) 2 pages.

A.S. Tanenbaum, et al.: Using Sparse Capability in a Distributed Operating System (1986) Proc. Sixth Int’l Conf. On Distributed Computing Systems, IEEE, pp. 558–563.

Robert D. Sansom, et al.: Extending a Capability Based System into a Network Environment (1986) Research sponsored by DOD, pp. 265–274.

List of Ameoba Papers, 3 pages.

Robert van Renesse, et al.: Wide–Area Communication Under Amoeba (Dec. 1986) IR–117, Vrije Universiteit, pp. 114–126.

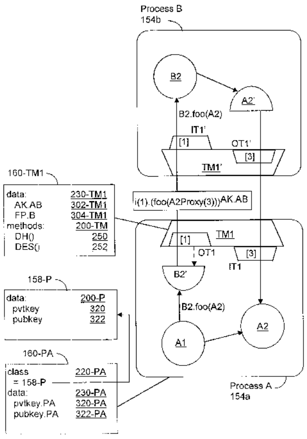
(List continued on next page.)

Primary Examiner—Alvin E. Oberley
Assistant Examiner—Peter Stecher
Attorney, Agent, or Firm—Pennie & Edmonds LLP

[57] **ABSTRACT**

A system and method is disclosed that provides persistent capabilities for distributed, object-oriented applications running on generally available hardware. The disclosed system and method operate in a transparent distributed object system where inter-process messaging between the program objects is effected by paired transport managers, proxies and matched in-table and out-table slots. Each object needing to communicate with an object in another address space does so by transparently issuing messages to that object’s local proxy. Each process provides a registrar that includes a secret code table wherein an object is registered with a unique, practically unguessable secret code. Anticipating the need to re-establish object-proxy links following a inter-process communications fault, proxies are made revivable, meaning that their links with corresponding remote objects can be revived following a communications interruption. This is accomplished by a makeRevivable method that stores a revivable proxy’s expiration date (the date beyond which the proxy is not revivable) and its corresponding remote object’s secret code into the proxy’s out-table slot. Upon the occurrence of a communications fault, all transport managers and tables are nulled out and then, when the communications fault is corrected, rebuilt by the transport managers. Sometime after the restoration of communications, a revived method is invoked that restores the links between, registered objects and proxies. The objects and proxies are brought back in a consistent state based on limited checkpointed data stored by the distributed program for the registered objects.

18 Claims, 12 Drawing Sheets



United States Patent [19]

Hellman et al.

[11] **4,424,414**

[45] **Jan. 3, 1984**

[54] **EXPONENTIATION CRYPTOGRAPHIC APPARATUS AND METHOD**

[75] Inventors: **Martin E. Hellman,** Stanford, Calif.; **Stephen C. Pohlig,** Acton, Mass.

[73] Assignee: **Board of Trustees of the Leland Stanford Junior University,** Stanford, Calif.

[21] Appl. No.: **901,770**

[22] Filed: **May 1, 1978**

[51] **Int. Cl.³** **H04K 9/00**
[52] **U.S. Cl.** **178/22.11;** 178/22.1; 178/22.14
[58] **Field of Search** .... 178/22, 22.1, 22.11, 178/22.14; 179/1.5 R

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,079,188 3/1978 Kinch, Jr. et al. 178/22

OTHER PUBLICATIONS

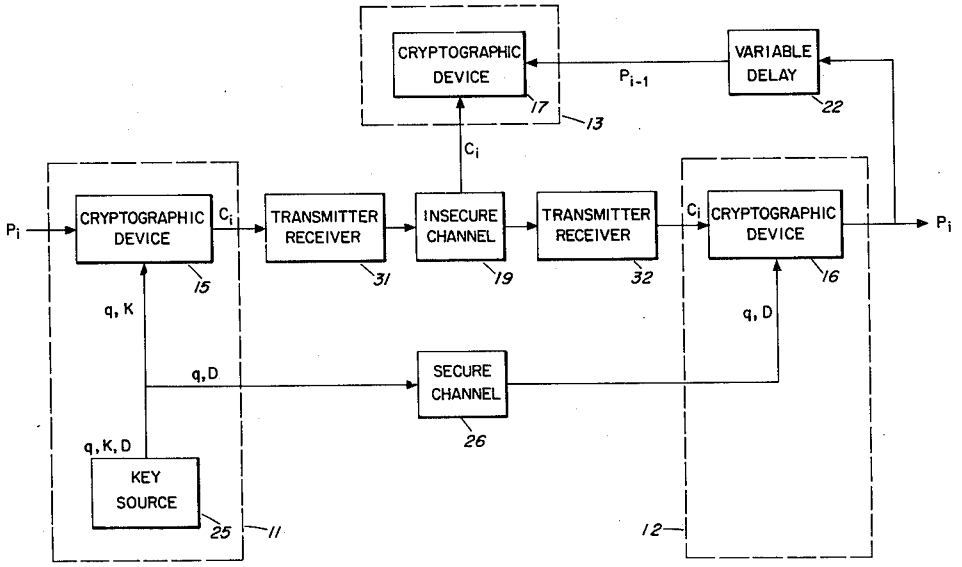
"New Directions in Cryptography", Hellman et al., *IEEE Transactions on Information Theory,* vol. IT-22, No. 6, Nov. 76, pp. 644–654.
"Multiuser Cryptographic Techniques", Diffie et al., *AFIPS-Conference Proceedings,* vol. 45, pp. 109–112, Jun. 1976.

Primary Examiner—Sal Cangialosi
Attorney, Agent, or Firm—Flehr, Hohbach, Test, Albritton & Herbert

[57] **ABSTRACT**

A cryptographic system transmits a computationally secure cryptogram that is generated from a secret transformation of the message sent by the authorized transmitter; the cryptogram is again transformed by the authorized receiver using a secret reciprocal transformation to reproduce the message sent. The secret transformations use secret cipher keys that are known only by the authorized transmitter and receiver. The transformations are performed with nonsecret operations, exponentiation, that are easily performed but extremely difficult to invert. It is computationally infeasible for an eavesdropper either to solve known plaintext-ciphertext pairs for the secret cipher keys, or to invert the nonsecret operations that are used to generate the cryptogram.

2 Claims, 6 Drawing Figures



United States Patent [19] [11] **4,200,770**

Hellman et al. [45] **Apr. 29, 1980**

[54] **CRYPTOGRAPHIC APPARATUS AND METHOD**

[75] Inventors: **Martin E. Hellman,** Stanford; **Bailey W. Diffie,** Berkeley; **Ralph C. Merkle,** Palo Alto, all of Calif.

[73] Assignee: **Stanford University,** Palo Alto, Calif.

[21] Appl. No.: **830,754**

[22] Filed: **Sep. 6, 1977**

[51] **Int. Cl.**^{2} **H04L 9/04**

[52] **U.S. Cl.** .... **178/22;** 340/149 R; 375/2; 455/26

[58] **Field of Search** .... 178/22; 340/149 R

[56] **References Cited**

PUBLICATIONS

"New Directions in Cryptography", Diffie et al., *IEEE Transactions on Information Theory,* vol. IT–22, No. 6, Nov. 1976.

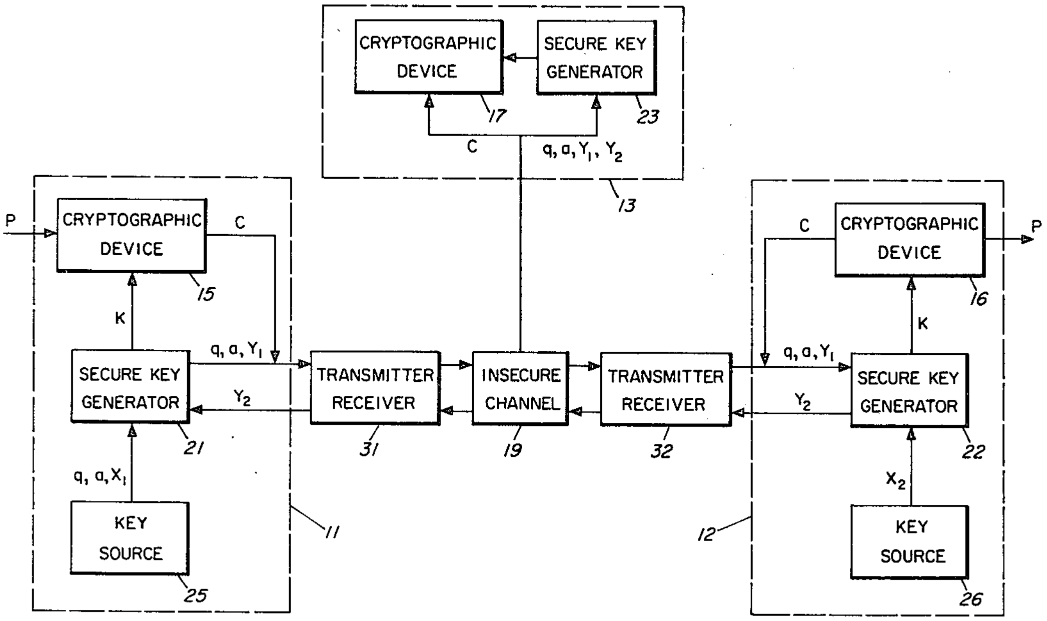
Diffie & Hellman, Multi–User Cryptographic Techniques", *AFIPS Conference Proceedings,* vol. 45, pp. 109–112, Jun. 8, 1976.

Primary Examiner—Howard A. Birmiel
Attorney, Agent, or Firm—Flehr, Hohbach, Test

[57] **ABSTRACT**

A cryptographic system transmits a computationally secure cryptogram over an insecure communication channel without prearrangement of a cipher key. A secure cipher key is generated by the conversers from transformations of exchanged transformed signals. The conversers each possess a secret signal and exchange an initial transformation of the secret signal with the other converser. The received transformation of the other converser's secret signal is again transformed with the receiving converser's secret signal to generate a secure cipher key. The transformations use non-secret operations that are easily performed but extremely difficult to invert. It is infeasible for an eavesdropper to invert the initial transformation to obtain either conversers' secret signal, or duplicate the latter transformation to obtain the secure cipher key.

8 Claims, 6 Drawing Figures



United States Patent [19] [11] **4,218,582**

Hellman et al. [45] **Aug. 19, 1980**

[54] **PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD**

[75] Inventors: **Martin E. Hellman,** Stanford; **Ralph C. Merkle,** Palo Alto, both of Calif.

[73] Assignee: **The Board of Trustees of the Leland Stanford Junior University,** Stanford, Calif.

[21] Appl. No.: **839,939**

[22] Filed: **Oct. 6, 1977**

[51] **Int. Cl.**^{2} **H04L 9/04**
[52] **U.S. Cl.** **178/22;** 364/900
[58] **Field of Search** 178/22

[56] **References Cited**

PUBLICATIONS

"New Directions in Cryptography," Diffie et al., *IEEE Transactions on Information Theory,* vol. II22, No. 6, Nov. 1976, pp. 644–654.

"A User Authentication Scheme not Requiring Secrecy in the Computer," Evans, Jr., et al., *Communications of the ACM,* Aug. 1974, vol. 17, No. 8, pp. 437–442.

"A High Security Log–In Procedure," Purdy, *Communications of the ACM,* Aug. 1974, vol. 17, No. 8, pp. 442–445.

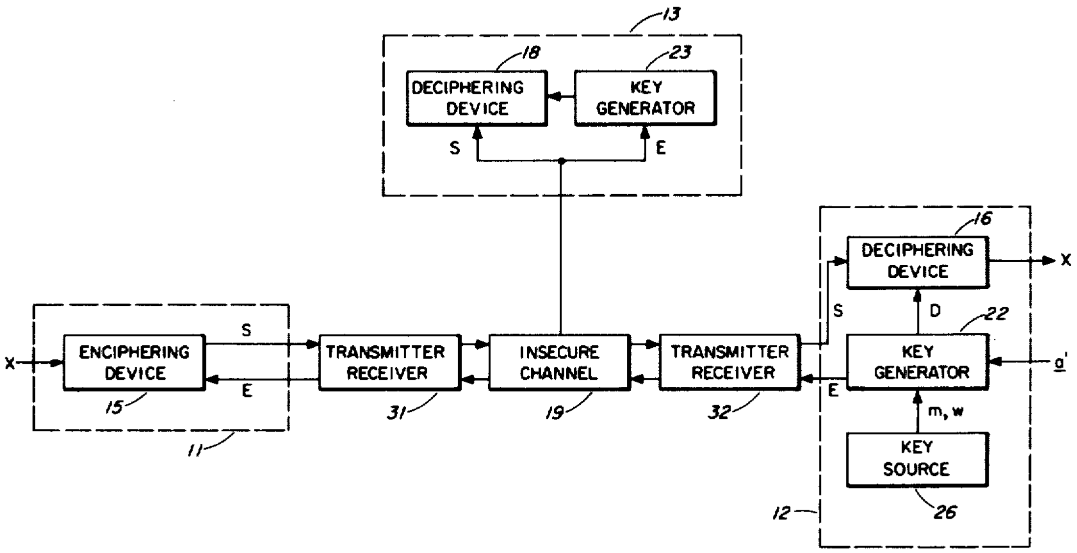
Diffie et al., "Multi–User Cryptographic Techniques," *AFIPS Conference Proceedings,* vol. 45, pp. 109–112, Jun. 8, 1976.

Primary Examiner—Howard A. Birmiel

[57] **ABSTRACT**

A cryptographic system transmits a computationally secure cryptogram that is generated from a publicly known transformation of the message sent by the transmitter; the cryptogram is again transformed by the authorized receiver using a secret reciprocal transformation to reproduce the message sent. The authorized receiver's transformation is known only by the authorized receiver and is used to generate the transmitter's transformation that is made publicly known. The publicly known transformation uses operations that are easily performed but extremely difficult to invert. It is infeasible for an unauthorized receiver to invert the publicly known transformation or duplicate the authorized receiver's secret transformation to obtain the message sent.

17 Claims, 13 Drawing Figures


13
18
23
DECIPHERING DEVICE
KEY GENERATOR
S
E
16
DECIPHERING DEVICE
X
S
D
22
KEY GENERATOR
a'
X
ENCIPHERING DEVICE
S
E
15
11
TRANSMITTER RECEIVER
31
INSECURE CHANNEL
19
TRANSMITTER RECEIVER
32
E
m, w
KEY SOURCE
26
12